REINALDO LEOPOLDINO CAVALCANTI JR.

ENGENHARIA SOCIAL NAS REDES SOCIAIS

Monografia apresentada ao Departamento de Informática (DIN) da Universidade Estadual de Maringá (UEM) como parte dos requisitos para obtenção do título de Especialista em Desenvolvimento de Sistemas para Web.

Prof. Dra. Luciana Andréia Fondazzi Martimiano
(Orientadora)

Maringá-PR

2011

“A eficácia de um sistema de segurança é medida pelo elo mais fraco da corrente”,

Kevin Mitnick

Esta monografia é dedicada à Vanessa Olivia Chiarelli, que eu reencontrei por meio do Orkut depois de 16 anos e hoje é minha esposa.

AGRADECIMENTOS

A produção desta monografia contou com a ajuda inestimável de diversas pessoas. Em primeiro lugar, ao coordenador do curso de Especialização em Desenvolvimento de Sistemas da UEM, Wesley Romão, por ter dado a oportunidade a um jornalista "*webdesigner*" de fazer parte de uma turma formada por profissionais veteranos em informática. Em segundo, lugar à minha orientadora, Luciana Martimiano por me ensinar como se faz uma monografia e evitar que tudo isso aqui ficasse com cara de jornal. Em terceiro, aos meus pais e sogros, pelo apoio financeiro, logístico e moral durante um ano e meio de longas viagens de madrugada para chegar e voltar de Maringá. Aos meus companheiros de sala, pelas incontáveis noites de cerveja e pizza, onde eram ensinados os "macetes digitais" que nenhuma sala de aula ensina. Aos professores, por terem suportado a interminável enxurrada de perguntas óbvias e deslocadas da realidade com bom humor e paciência. E por último, mas não menos importante, à minha esposa, Vanessa Chiarelli, pelo amor, apoio, paciência e dedicação durante toda a duração do curso.

RESUMO

Os serviços de redes sociais, como o Orkut, encontraram terreno fértil entre os internautas brasileiros. Combinando o crescimento econômico do país, o acesso do público à tecnologia mais barata e a natureza social do povo brasileiro, esses sites se tornaram um dos destinos mais visitados na Internet do país. Mas com a novidade da tecnologia também veio o perigo: criminosos virtuais, usando técnicas psicológicas avançadas chamadas de engenharia social, vasculham perfis sociais mal protegidos para obter informações pessoais e privadas para usá-las contra suas vítimas em crimes como truques de confiança, furto ou roubo de identidade. O objetivo deste estudo é analisar este problema, e propor uma possível solução para evitar este tipo de falha de segurança que não está relacionada à tecnologia em si, mas é inerente ao comportamento humano.

Palavras Chaves: Engenharia Social, Redes Sociais, Segurança

ABSTRACT

Social Networking Services, like Orkut, took Brazilian Internet users like a storm. Combining the economic growth of the country, the public's access to cheaper technology and the social nature of the Brazilian people, these web services became one of the most visited destinies over the country's Internet. But with the novelty of the technology also came danger: cyber criminals, using advanced psychological techniques called social engineering, scavenged poorly secured social profiles for personal and private information to use against their victims in crimes as confidence tricks, burglary and identity theft. The aim of this study is to analyze this problem, and propose a possible solution to avoid this type of security breach that is unrelated to the technology, but inherent to the human behavior.

Keywords: Social Engineering, Social Networks, Security

LISTA DE GRÁFICOS

LISTA DE IMAGENS

SUMÁRIO

1. INTRODUÇÃO

As redes sociais ou sites de relacionamentos podem ser considerados, hoje, uma das ferramentas mais versáteis para fazer amigos, manter contatos e conhecer pessoas por meio da Internet. A cada dia, mais usuários da web fazem parte dessas redes, graças ao baixo custo dos equipamentos de informática e de acesso à conexão, como também por projetos de inclusão digital.

Sites como Orkut, Facebook, Twitter, que possuem um grande número de usuários, oferecem diversas ferramentas que facilitam as interações sociais de seus membros. Seus usuários podem criar álbuns de fotos personalizados, perfis com uma enorme gama de informações pessoais, comunidades nas quais os membros podem discutir sobre temas de mútuo interesse etc.

Tais informações normalmente são de domínio público, a não ser que o usuário em questão restrinja o acesso das mesmas para serem compartilhadas apenas com seu círculo de amigos reais.

Para os membros que não fazem parte desse círculo de amizade, poucas são as informações as quais se possui acesso, criando assim, uma "zona de segurança" contra usuários desconhecidos.

Entra em cena a Engenharia Social. Segundo Kevin Mitnick (2004), um Engenheiro Social é uma pessoa que manipula a confiança de outra para ter acessos a informações consideradas privadas. Ele também pode, por meio das poucas informações a que tem acesso, montar um quadro mais aprofundado de um alvo. Sem que o alvo saiba, essas informações que ele considera irrelevantes dão ao engenheiro social a possibilidade de prejudicar seu alvo empresarialmente, socialmente, financeiramente ou psicologicamente.

Nesta primeira década do século XXI, houve um aumento considerável de ataques que envolvem engenharia social que partiram de redes de relacionamentos. Ataques como *phishing* (o usuário é ludibriado para acessar um site falso de uma instituição financeira), roubo de identidades, roubo de senhas bancárias, *stalking* (perseguição virtual ou física de um alvo) tem se tornado um verdadeiro desafio para os responsáveis pela segurança dessas redes.

O desafio está no fato de que o problema não reside na parte tecnológica dos sites, mas sim no "fator humano". Seja por inexperiência com uma nova tecnologia ou pelo instinto inerente de se socializar, são os próprios usuários que põe suas informações em risco.

O objetivo principal deste trabalho é analisar este problema, definindo quais são as principais áreas de risco as quais os usuários estão expostos. Além disso, definir por meio de dados levantados, estatísticas e estudos de casos, quais são os principais ataques arquitetados pelos engenheiros sociais e como esses ataques tem atingido os usuários de redes sociais. Por fim, por meio dessa análise, estudar as estratégias de segurança que os responsáveis dessas redes usam para reduzir este problema em seus sites.

No intuito de alcançar esses objetivos, esta monografia foi dividida em sete diferentes capítulos. No Capítulo 2, são descritos os objetivos gerais e específicos sendo acompanhados, no Capítulo 3, pela justificativa geral da execução deste trabalho.

O Capítulo 4 apresenta a fundamentação teórica, bem como os direcionamentos necessários para a aplicação prática deste trabalho. O Capítulo 5 descreve a evolução do processo de segurança nas redes sociais. No Capítulo 6, a metodologia é descrita em detalhes com os passos que foram realizados para a execução da experimentação prática.

Por fim, o Capítulo 7 descreve detalhadamente o processo de experimentação e a análise dos dados. Este capítulo é seguido pelo capítulo final, a Conclusão, na qual tudo o que foi discutido neste estudo é resumido e algumas soluções são apresentadas.

1.1 Objetivos

Tendo em vista a natureza instintivamente social do problema da exposição online, este estudo não pretende encontrar uma solução definitiva para o problema da engenharia social. Do ponto de vista acadêmico, ele pretende, na verdade, traçar linhas de ação para minimizar a exposições de informações pessoais sigilosas dos usuários dentro das redes sociais.

Devido à vasta quantidade de sites de relacionamentos, o foco deste projeto estará restrito ao Orkut. Segundo o site Alexa.com, 56,3% dos usuários do Orkut são brasileiros, tornando-o a rede social mais utilizada no país (ALEXA, 2011).

Dentro dessa prerrogativa, pode-se dizer que os objetivos específicos deste projeto são:

- Executar um levantamento estatístico dentro de perfis pessoais, visando a definir padrões nos dados que os usuários liberam para divulgação pública.
- Realizar levantamento literário (em livros, jornais e revistas) sobre situações em que a Engenharia Social foi utilizada para prejudicar um ou mais usuários de sites de relacionamento.
- Definir os tipos de ataques mais utilizados pelos Engenheiros Sociais.

1.2 Justificativa

A necessidade humana de se socializar não é recente. Desde as primeiras tribos, os seres humanos se aglomeravam em grupos como forma de sobrevivência. A recente explosão digital e o acesso dos humanos a uma rede de comunicação interligada de proporções globais trouxeram toda uma mudança no paradigma do que é fazer parte de um grupo.

Os sites de relacionamento são apenas um reflexo dessa necessidade. Oferecendo aos seus usuários uma gama diversa de possibilidades de fazer amigos, conhecer pessoas e refinar o relacionamento com contatos já existentes, não é de se espantar que as redes sociais sejam listadas atualmente como os sites mais visitados da Internet.

O problema da Engenharia Social também não é recente, mas encontrou nesses sites um terreno fértil onde um usuário mal intencionado pode obter informações privadas com facilidade e de forma anônima.

Gostos pessoais, endereços, números de telefones, fotos de famílias, de viagens, de eventos, tudo pode ser acessado com apenas poucos cliques. Por meio dessas informações, amizades podem ser estabelecidas, negócios podem ser feitos, relacionamentos podem desabrochar. No entanto, do outro lado da moeda, um usuário mal intencionado, um engenheiro social, pode utilizar esses dados para prejudicar um usuário idôneo de diversas maneiras.

A chegada da segunda década do século XXI viu um enorme aumento dos números de *confidence tricks*, ou ataques de confiança, nos quais um criminoso virtual comete crimes se baseando apenas na inexperiência ou da necessidade de se socializar dos outros usuários.

Seja no meio empresarial, na vida pessoal, financeira ou romântica, os danos causados por um ataque bem arquitetado pode colocar em risco a segurança de um usuário inexperiente.

Partindo do pressuposto de que todo ser humano precisa se socializar, evitar esse tipo de ataque nas redes sociais é de grande importância.

A prerrogativa básica deste estudo é analisar este processo. O problema da engenharia social não é de fácil solução, por conta dessa necessidade básica dos seres humanos de fazer parte de uma comunidade, de um grupo social.

O que este trabalho pretende fazer é entender como esses ataques acontecem e por meio de dados estatísticos, definir as áreas de maior problema nas redes de relacionamento. De posse dessas informações, pretende-se definir estratégias para reprimir este tipo de ataque ou ao menos, reduzir os danos aos quais os usuários estão expostos.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 A origem e a expansão das Redes Sociais Digitais

Apesar do conceito atual de "rede social digital" ter surgido no começo da primeira década do séc. XXI com os sites de relacionamentos Makeoutclub.com (2000) e o Friendster.com (2002), a ideia de comunidade digital é bem mais antiga. Com base na necessidade humana de socialização e interação, os primeiros passos da evolução da Internet sempre caminharam juntos com o ideal de juntar pessoas e formar grupos.

Mesmo no final do século passado, quando os microcomputadores ainda engatinhavam em direção a uma hegemonia domiciliar, alunos e acadêmicos dentro de universidades e centros de pesquisas já utilizavam redes de emails como a Usenet (1980) e BBS (1979) para se comunicar em grupo. É fato que, em termos comparativos, tanto a interface, quanto a usabilidade e a quantidade de informações disponíveis sobre um usuário diferiram radicalmente com o passar do tempo, porém o conceito e a relevância dessas redes mais antigas são as mesmas se comparadas proporcionalmente com as de vinte anos depois.

Quando Michael e Ronda Hauben escreveram o livro *Netizens* em 1995, discutindo os impactos das "redes sociais" da época na sociedade humana, eles não pouparam exemplos de "inovações" nos relacionamentos sociais digitais que hoje é tomado por corriqueiro. Segundo os autores, "...as conexões sociais que antes nunca seriam possíveis, ou relativamente difícil de serem feitas, agora foram facilitadas pela Net. O tempo e a geografia deixaram de ser obstáculos" (HAUBEN e HAUBEN, 1995).

Eles afirmam, ainda, que graças a esse novo meio de comunicação, "...as limitações sociais e convenções não mais evitam uma potencial relação ou parceria" e declaram que "agora, as pessoas tem o poder de transmitir suas observações ou questões por todo mundo e receber respostas de outras pessoas. As redes de computadores formam uma nova conexão de base que permite setores excluídos da sociedade terem uma voz ".

É possível perceber que já na década de 90, na qual gigantes sites de relacionamento como Facebook, Twitter ou o Orkut nem existiam, o conceito de comunidade virtual já estava presente e em pleno funcionamento, apesar das dificuldades técnicas da época.

Essas dificuldades, nas quais se enquadram velocidade de transmissão, capacidade de processamento e armazenamento, foram suplantadas com o passar do tempo, gerando oportunidades para que as redes de relacionamento virtuais oferecessem novas formas de interação entre os grupos. Aliando isso ao baixo custo para aquisição de tecnologia por parte dos usuários, o número de membros das comunidades virtuais cresceu exponencialmente.

Tendo em vista esses fatores, pode-se dizer que, conceitualmente, uma rede social digital é uma plataforma que permite a interação de pessoas por meio de grupos de discussão e relacionamento. Como dito no início desta seção, apesar desse conceito parecer recente, ele existe desde a década de 80 do sec. XX.

Porém, talvez o fato mais marcante dentro da evolução das redes sociais aconteceu com a mudança do foco das discussões em grupo para a criação de perfis pessoais. Esse novo formato se popularizou na primeira década do séc. XXI com o Friendster (KNAPP, 2006). Usuários podiam criar páginas pessoais dentro das redes de relacionamento que continham informações sobre gostos pessoais, perfis musicais, visões políticas e filosóficas. Esses perfis ganharam ainda mais relevância com a capacidade de *postar* fotos e criar listas de amigos, nas quais o usuário agregava ao seu perfil, links para os perfis de amigos, parentes e colegas de trabalho.

Essa mudança de foco para o lado pessoal do usuário transformou os grupos de discussão dentro de uma temática comum (como acontecia na Usenet) para grupos sociais de amigos em comum. Foi a partir daí que o conceito atual de rede social como é conhecido hoje ganhou seu *momentum*.

Quando os gigantes das redes sociais começaram a surgir na primeira década do séc. XXI, a importância do "perfil pessoal" foi o fator que mais impulsionou a expansão dos sites de relacionamento. Segundo Ellison *et al.* (2009), no seu artigo *A networked self,* "as redes sociais nos permitem representar digitalmente nossas conexões com outros usuários - o que significa que podemos usar esses sites para modelar nossa rede social de relacionamentos".

Para os autores, essa capacidade de virtualizar o "eu" das mais diversas formas dentro de uma rede social é o que fez os sites de relacionamento uma ferramenta tão cotidiana na vida da sociedade atual: "O que verdadeiramente distingue sites de redes sociais de tecnologias anteriores é a rede social articulada que é o centro desses sistemas."

Foi partindo dessa premissa de redes sociais centradas em *redes de amigos*, que houve um florescimento e expansão dos sites de relacionamento na primeira década do séc. XXI.

O já citado Friendster surgiu em 2002 e hoje conta com 90 milhões de usuários, a maior em países asiáticos. O hi5 veio em 2003, sendo bastante popular na europa e no oriente médio, com 80 milhões. No mesmo ano surgiram o Myspace e o Linkedln, este último com o foco em contatos profissionais e de negócios. Atualmente, ambas as rede possuem mais de 100 milhões de usuários demograficamente centrado na América do Norte. No entanto, foi em 2004 que surgiu a maior rede social de todas: o Facebook. Atualmente, apenas esta rede possui mais de meio bilhão de usuários espalhados por todas as regiões do planeta.

Variações de sites de relacionamento dentro de uma temática central como o deviantArt (artístico), o Flickr (fotografia), o Last.fm (música) e o Twitter (*microblogging*) também ganharam força e hoje contam com centenas de milhares de usuários registrados.

No Brasil, a rede social que mais ganhou destaque e o maior número de adeptos foi o Orkut. Apesar de esta rede possuir mais de 100 milhões de usuários registrados de diversas partes do mundo, a grande maioria é de brasileiros. Na próxima seção, é discutida a evolução desta rede no Brasil.

2.2 A hegemonia do Orkut no Brasil e seu impacto social

O Orkut surgiu em 2004 durante o crescimento das redes sociais centradas em perfis pessoais. Seu nome é uma referência direta ao nome do criador do projeto, o funcionário da Google Orkut Büyükkökten. Como todas as redes dessa época, grande parte do tráfego de usuários provinha dos Estados Unidos. Segundo o site Alexa.com que compila estatísticas de visitação, em 2004, 50% dos usuários eram americanos (ALEXA, 2011).

No entanto, com o passar dos anos, o fluxo de usuários migrou essencialmente para dois países: Brasil e Índia. Em 2010, o site de relacionamentos já era o 11º mais visitado do Brasil e dos seus 100 milhões de usuários registrados, 57% eram brasileiros (ALEXA, 2011). Assim, é possível dizer que pelo menos um quarto da população brasileira possuiu em algum momento um perfil pessoal no Orkut.

O editor do site IDG Now!, Guilherme Felitti, afirma em artigo datado de 2008, que a razão para esse sucesso entre os brasileiros se deveu a três fatores principais: primeiro, a falta de concorrência do Orkut na época do seu lançamento, segundo, a usabilidade do site era

simples e eficiente, ao contrário de outros sites da época, como o Myspace. A terceira razão, no entanto, veio por conta da estratégia de marketing. No seu lançamento, apenas era possível criar um perfil no site quem tivesse sido convidado (FELITTI, 2008).

Segundo o Felitti, "...a necessidade de um convite para participar, o que instigava a curiosidade dos que ainda estavam de fora para entender qual era o grande atrativo da rede social." Para o autor, "Isso agiu como uma espécie de fermento para a vontade do internauta em fazer seu perfil."

O próprio criador do site, em entrevista à Revista Folha de 2005, confirma o terceiro ponto citado por Felitti, mas também afirma que o sucesso pode ter vindo de questões sociais: "Talvez seja cultural, tenha a ver com a personalidade de vocês, que são conhecidos como um povo amigável" (FOLHA ONLINE, 2005).

Em 2010, o site de estatísticas comScore afirmou que de cada quatro internautas brasileiros, três tinham perfis no Orkut: "Em agosto de 2010, mais de 36 milhões de usuários de Internet visitou um site de relacionamentos no Brasil. O Orkut é classificado como o destino mais visitado, atingindo 29,4 milhões de visitantes" (COMSCORE, 2010).

Essa hegemonia dentro de um país como o Brasil, que ainda engatinha no sentido da inclusão digital e que possui uma enorme desigualdade social, fez do Orkut se estabelecer no país como a principal rede de relacionamento e um item quase que indispensável na navegação diária do usuário comum brasileiro.

Na próxima seção, são discutidas as características principais das redes sociais e as ferramentas que os usuários dispõem nesses sites para fazer amigos e formar grupos.

2.3 Características e tendências das redes sociais

Como dito na primeira seção, as características marcantes dos sites de relacionamento mudaram de foco com o passar dos anos. A atenção ao "perfil pessoal" fez surgir diversas ferramentas e implementações que permitiram aos usuários disponibilizar mais informações pessoais das mais diversas maneiras.

A análise dessas características é fundamental na compreensão do atual cenário no qual ocorre a intercomunicação dos usuários. Apesar do escopo deste estudo ser o site de relacionamento Orkut, todas ou quase todas as características discutidas a seguir são comuns às maiores redes sociais da Internet.

O **Perfil Pessoal** é o ponto de entrada principal dos usuários. Nele, o usuário encontra sua lista de contatos, suas comunidades afiliadas, as atualizações feitas nos perfis de amigos, seu álbum de fotos e vídeos e sua página de *scraps* (mensagens curtas enviadas por outros usuários para o seu perfil).

A finalidade do perfil, como o nome já diz, é traçar um perfil do usuário a partir de informações que ele disponibiliza, como seu status de relacionamento (solteiro, casado etc), sua data de aniversário, seu email pessoal, endereço residencial, cidade, estado. Além disso, o perfil permite ao usuário informar gostos pessoais e hábitos relevantes à formação de grupos de amigos como gosto musical, religião do usuário, opção sexual, livros que gosta de ler, hábitos de saúde e prática de esporte.

Há também a possibilidade de informar dados trabalhistas e acadêmicos como empresas trabalhadas, ramos de atuação, escolas e cursos feitos etc. Por fim, há uma última área na qual o usuário pode informar traços físicos como cor do cabelo, dos olhos, a presença de tatuagens ou *piercings*, etc.

A variedade de detalhes pessoais possíveis de se informar num perfil social cresceu com o passar dos anos, chegando ao patamar atual em que quase todos os traços de personalidade podem ser informados e divulgados para a rede.

Por meio dessas informações, teoricamente, novos amigos poderão ter uma ideia de quem o usuário é, do que ele gosta e se existe uma compatibilidade entre as duas pessoas. É também por meio desses dados que os mecanismos internos do site de relacionamento pesquisam outros perfis à procura de traços de personalidade em comum e informa ao usuário as possíveis compatibilidades entre ele e novos usuários, sob o título de *Sugestão de Amigos*.

Seu ***scrapbook***, ou caixa de mensagens, é onde o usuário encontra todo o histórico de mensagens trocadas entre ele e os outros usuários da rede. O que antes era apenas um lugar onde mensagens apareciam, hoje assumiu o formato de *conversas*, onde as mensagens são agrupadas por usuários e por data, possibilitando uma compreensão melhor do fluxo de conversação entre duas pessoas. Todos os membros pertencentes à lista de amigos do usuário podem ver parcial ou completamente o seu histórico de conversas.

O **álbum de fotos e vídeos** surgiu com o aumento da banda de transmissão pela Internet. Por meio dele os usuários possuem um espaço virtualmente infinito para divulgar fotos e vídeos pessoais. Esses elementos *multimídia* podem ser agrupados em grupos

temáticos e ter permissões atribuídas a eles, definindo quais pessoas da rede social pode ter acesso e visualizá-los. Normalmente, a permissão padrão para novos itens adicionados é "apenas para amigos", porém esse status pode ser modificado para atingir um grupo menor ou maior de pessoas.

Uma implementação recente ao álbum de fotos é a capacidade de adicionar *tags* (ou marcadores) nas imagens, informando o link do perfil das pessoas que estavam presentes naquela foto. Isso cria um elo entre o álbum de fotos e o perfil pessoal de outro usuário.

As **comunidades** servem como um vínculo ao modelo antigo das redes sociais de grupos de discussão. Nelas o usuário normalmente discute assuntos relacionados aos temas da comunidade com outros membros, criando assim, uma lista de discussão similar aos *fóruns*, que qualquer membro da rede tem acesso.

Atualmente, o número de comunidades dentro do Orkut supera os milhões. Elas estão divididas nas mais variadas temáticas como Artes e Entretenimento, Negócios, Países e Regiões, Culturas e Comunidade, Família e Lar, Moda e Beleza, Culinária entre outros. Existe também um enorme número de "comunidades de afirmação" que não pertencem a nenhum grupo específico, mas tem como meta juntar usuários que possuem características pessoais em comum como "*odiar acordar cedo*", "*adorar lasanha*", "*ser ciumento*", "*enrolar nas tarefas domésticas*", "*procrastinar no trabalho*" entre outros.

Este último grupo de comunidades voltará a ser discutido mais à frente. No entanto, primeiro, são discutidos os principais problemas de segurança que atingem os usuários do Orkut e por consequência os usuários das redes sociais em geral.

2.4 Os problemas de segurança das redes sociais

Como toda nova tecnologia implementada e passiva de falhas, os sites de relacionamento tiveram ao longo dos anos diversos problemas com segurança. O rápido crescimento da base de usuários, a concorrência entre as diversas redes e a corrida para lançar uma nova ferramenta ou um novo recurso dentro desses sites, fizeram com que, a cada ano, mais e mais usuários sofressem por conta de roubo de informações e falhas na proteção à privacidade (COLLINS, 2008).

Esses problemas com segurança se agravaram de diversas formas com o passar do tempo e com o aumento dos usuários de sites de relacionamento. As falhas vão desde a quebra

de privacidade, o roubo de dados, o acesso a informações privadas por empresas de marketing, ataques de vírus e de engenheiros sociais (COLLINS, 2008).

Apesar do escopo deste projeto ser o site de relacionamentos Orkut, as falhas discutidas nesta seção são comuns em quase todas as outras redes sociais.

Segundo Barnes (2006) discute no seu artigo *A Privacy Paradox*, a mudança de foco das redes para os perfis pessoais também foi precursora de um dos maiores problemas enfrentados pelos usuários de sites de relacionamento: a quebra de privacidade.

Com a possibilidade de postar textos, fotos, vídeos ou deixar comentários e depoimentos, os membros dessas redes viram nos sites de relacionamento uma plataforma prática e rápida de divulgação pessoal. Essa divulgação não significa necessariamente uma propaganda pessoal, mas sim uma parte do processo de fazer novos amigos e conhecer novos grupos sociais (BARNES, 2006).

No entanto, esse fluxo de informações pessoais era acessível, até pouco tempo atrás, a todos os usuários da rede independentemente se havia ou não algum vínculo entre dois usuários em comum. Isso significa que tudo que era postado, discutido, comentado ou dito por um usuário, podia ser plenamente acessado por qualquer membro da rede. A única barreira que existia era apenas ser ou não usuário da rede social.

Segundo Bornatovsky (2006), o problema é que "muitos usuários, de certa forma, confiam cegamente [nessas redes], muitas vezes por falta de conhecimento, disponibilizando todos os seus dados pessoais e fotos". Para ele o problema se agrava, pois preenchendo campos preestabelecidos e não obrigatórios que traçam completamente o chamado “perfil do usuário”, os participantes dos sites de relacionamento não se davam conta de que essas informações podiam ser acessadas por qualquer usuário que também tenha um perfil cadastrado.

São inúmeros os casos noticiados nos quais essa divulgação pessoal e o acesso total a informação por parte dos outros membros da rede se tornou prejudicial aos usuários. Casamentos foram desfeitos, empregos foram perdidos, amizades foram separadas simplesmente por que a "outra parte" teve acesso demais a informações privadas de um determinado usuário.

Essa exposição total de dados privados e pessoais também se tornou uma ferramenta para criminosos praticarem crimes, por exemplo. Em notícia datada de 23/04/2006, o jornal online 24HorasNews cita casos nos quais falsos sequestradores se utilizam de informações divulgadas pelas vítimas nos seus perfis pessoais para enganar parentes e amigos:

> "Pelo Orkut, os marginais sabem, por exemplo, onde a vítima em potencial combinou de ir à noite e, de posse dessa informação, podem ligar para os familiares para simular o falso sequestro. Além disso, os bandidos têm como saber o círculo social da pessoa e o padrão de vida, como quantos carros e imóveis ela tem, facilitando na hora de enganar os familiares." (24HorasNews, 2006).

Além disso, mas num âmbito não criminal, há também a questão da mineração de dados (*data mining*), executado pelas empresas de marketing. Utilizando as ferramentas de buscas incluídas nos próprios sites de relacionamentos, essas empresas procuravam por palavras chaves nos perfis e nas comunidades afiliadas do usuário, para traçar um perfil de um possível cliente (ELKINS, 2007).

A partir desses dados, as empresas utilizavam os próprios espaços de comunicação pessoal (os *scraps* do Orkut) para fazer propagandas dos seus produtos. Não eram raros os casos de empresas que se utilizavam da prática do *spam* (emails de propaganda não solicitados) para atingir os usuários (ELKINS, 2007).

Outro problema bastante corriqueiro nas redes sociais eram os vírus. Durante a fase de expansão dos sites de relacionamento, a quantidade de tecnologias novas implementadas abria espaço para falhas de segurança que permitiam criminosos virtuais disseminar programas maliciosos como vírus, cavalos de troia (*trojans*) e *spywares.* A técnica mais simples era infectar um usuário e deixar o vírus se apoderar da sua lista de contatos para espalhar mensagens contendo o vírus. Como essas mensagens provinham de um usuário conhecido da lista, os outros usuários acreditavam que aquela era uma mensagem autêntica e clicava nos links anexados.

O texto das mensagens também era de cunho enganoso, mascarando o verdadeiro conteúdo dos links. "*Veja as fotos que nós tiramos no verão!*", "*Olha o que eu achei sobre você na net*" ou "*Olha só a nova música de [cantor famoso]*" são exemplos de frases automáticas que os vírus postavam.

No entanto, boa parte dos problemas citados foi resolvida ou minimizada extensamente com a consolidação do desenvolvimento desses sites. Novas tecnologias de segurança ou mudança nos processos dentro das redes sanaram a maior parte dos problemas.

A maior atenção foi dada a questão das permissões, ingrediente que faltava no painel de controle de boa parte dos sites de relacionamento. Com as permissões, os usuários podem agora escolher quem tinha acesso para ver seus *posts*, fotos, vídeos e comentários. Se um usuário quiser, por exemplo, ele pode ter um perfil pessoal extensamente povoado de informações pessoais, fotos e textos, mas apenas visíveis a um grupo de amigos íntimos. Os outros contatos, que também são colegas ou conhecidos do usuário, veem apenas parte dessas informações, pois sua permissão é de menor abrangência.

O problema dos vírus também foi minimizado com a implementação de *captchas*, conforme exemplos na Fig. 1, ou confirmações por escrito, que um usuário precisa interagir para postar mensagens com links anexos. Como essa interação normalmente requer uma leitura atenciosa dos *captchas,* a disseminação automática dos vírus perdeu bastante força.

Fig. 1: Exemplos de captchas usados pelo Orkut

No entanto, um dos problemas citados ainda não possui solução definitiva, pois de uma forma de outra, vai de encontro ao objetivo dos próprios sites de relacionamento: a questão da engenharia social. O que é a engenharia social, como se aplica e como ela tem se tornado um crescente problema nas redes sociais, serão os temas discutidos na próxima seção.

2.5 Engenharia social: a psicologia como ferramenta para o crime

O termo engenharia social se aplica a diversas técnicas que permitem a quem as utiliza conseguir acesso não autorizado a informações privadas e usá-las contra um alvo. O que isola a engenharia social como categoria única é o fato desse acesso ser conseguido por meio da psicologia contra o alvo (GOODCHILD, 2010).

O exemplo dos falsos sequestradores simplifica esse conceito: de posse de informações públicas e privadas, criminosos ligavam para as vítimas *simulando* um sequestro para conseguir um resgate. Não há sequestro propriamente dito e toda a simulação não passa de um engodo psicológico contra a vítima, que é reforçada pela posse de informações até então consideradas privadas.

No entanto, a técnica não se aplica apenas a falsos sequestros: fraudes, roubos de identidade, acessos não autorizado a sistemas de informações, *phishing*, entre outras práticas criminosas, se apoiam fortemente em engenharia social.

No livro *A Arte de Enganar*, o ex-*hacker* (hoje, consultor de segurança) Kevin Mitnick explica diversas situações nas quais o fator humano pode ser explorado pela engenharia social para obter informações privadas ou acesso a dados proibidos.

Em um dos exemplos, ele cita a situação na qual uma pessoa obtém acesso à intranet de uma empresa, mas que é protegida por uma senha que muda diariamente. Para descobrir a senha, ele aguarda por um dia de chuva forte, liga para empresa fingindo ser um empregado preso em casa por conta da tempestade e convence o operador a revelar a senha daquele dia.

Há também o caso no qual uma pessoa ganha acesso a uma área restrita de um local, ficando à porta dessa área carregando uma grande caixa de livros, e contando com a propensão das pessoas para manter a porta aberta para os outros nessa situação.

Os métodos variam de criminoso para criminoso, mas sempre são focados no lado psicológico da vítima. O próprio Mitnick passou cinco anos na prisão por crimes de roubo de informações e invasão de sistemas. Esses atos, segundo ele, foram cometidos utilizando técnicas de engenharia social para enganar pessoas fazendo-as acreditar ser alguém que ele não era.

Além dos dois exemplos citados, Mitnick cita métodos padrões que os engenheiros sociais usam para enganar suas vítimas, dentre eles estão:

- Entrar em contato com a vítima (empresa ou pessoa) fingindo ser um jornalista ou um escritor e fazer perguntas diversas sobre a empresa ou ramo de atuação, incluindo no meio das perguntas uma que extraia a informação que o criminoso deseja conseguir. Ex.: “Que

interessante! Mas durante a noite não aumentam os riscos de assalto? Como vocês cuidam dessa parte?”

- Entrar em contato com a vítima dizendo ser do banco, companhia elétrica, etc., requerendo informações para fazer um recadastramento da vítima no sistema. Ex.: “Sua conta de banco sofreu uma tentativa de invasão e precisamos que o Sr. confirme seus dados para poder desbloqueá-la”.

- Entrar em contato com a vítima dizendo ser de outro setor da mesma empresa que ela trabalha, para tirar “dúvidas” sobre um novo processo de segurança. Ex.: “Tá, a tela de *login* eu já entendi, mas eu não sei que senha essa que eles estão pedindo agora. Eles só fazem isso para complicar a nossa vida!”

Todos esses métodos possuem um único propósito: ganhar a confiança da vítima e fazê-la revelar uma informação confidencial que o engenheiro social precisa como parte do seu plano criminoso.

Segundo Laribee (2006), o ponto fraco de qualquer sistema de segurança, seja ele físico ou virtual, são as pessoas que fazem parte dele. É explorando a confiança dessas pessoas que um engenheiro social obtém acesso a informações restritas sem precisar lidar com o sistema de segurança em si.

Laribee (2006) cita, ainda, na sua dissertação de mestrado, uma pesquisa realizada em 2003 por uma empresa de segurança da Inglaterra, a InfoSec. Na pesquisa, funcionários de uma empresa preencheram um formulário com perguntas genéricas sobre o seu dia a dia no trabalho. Em troca, elas ganhariam uma caneta de brinde por ter respondido o questionário completo.

No meio do questionário havia a seguinte pergunta: Qual é a senha da sua estação de trabalho? Setenta e cinco porcento (75%) dos entrevistados responderam à pergunta. Quando questionados por que eles responderam essa pergunta, os funcionários disseram que foi por causa da caneta de brinde que quem respondesse o questionário ganhava (THE REGISTER, 2003).

Como é possível notar, o fator humano possui interferência fundamental na estabilidade de um sistema de segurança e um engenheiro social, com as técnicas certas, pode

comprometer esse sistema apenas forçando a confiança entre ele e a vítima. O problema é que, até o início desta década, os engenheiros sociais precisavam se expor para conseguir as informações das suas vítimas. No entanto, com o crescimento das redes sociais e o vasto número de usuários, esses criminosos encontraram um terreno fértil para seus levantamentos de dados, protegidos pelo anonimato da própria rede.

Na próxima seção é discutido como os engenheiros sociais se utilizam das ferramentas e recursos dos sites de relacionamento para obter informações confidenciais sobre suas vítimas.

2.6 Engenharia social em sites de relacionamento

A consolidação do uso das redes sociais entre os usuários de Internet abriu um novo espaço para o garimpo de informações por parte de um engenheiro social. Não mais dependente de se expor (ou pessoalmente ou por telefone) ou de deixar rastros (contato por email), um criminoso que se utiliza das técnicas citadas na seção anterior pode levantar dados sigilosos de uma vítima apenas visitando seu perfil social num site de relacionamento.

No artigo "*5 Things to Keep Off Social Networking Profiles*" (datado de 09/07/2010), a jornalista Jenniffer Mattern demonstra como os dados dos perfis sociais mostram muito mais sobre o usuário do que o próprio usuário imagina:

> "...muita gente não é tão cautelosa sobre o que coloca nesses perfis públicos. Eles realmente pensam que ninguém, apenas os seus amigos e contatos pessoais têm acesso à informação ali colocada. Então, eles postam coisas estúpidas sem pensar - coisas que podem custar-lhes o emprego..." (MATTERN, 2010).

No artigo MATTERN (2010) cita diversos pontos problemáticos de um perfil social, que podem expor dados sigilosos sobre um usuário sem que ele tenha consciência:

- Fotos comprometedoras ou provocativas – Fotos deste tipo colocam em risco a integridade do usuário e oferecem uma brecha à privacidade do usuário;
- Críticas aos amigos ou aos colegas de trabalho – Como a maioria dos comentários possui acesso global dos amigos do usuário, essas críticas podem chegar às pessoas a quem essa informação deveria permanecer sigilosa;

- Informações confidenciais – O que se passa dentro do trabalho ou de casa deve permanecer sigiloso, pois essas informações podem se tornar arma na mão de usuários mal intencionados;
- Dados pessoais – O usuário deve ter cuidado ao postar informações pessoais como endereço, local de trabalho, opção sexual, entre outros, pelas mesmas razões do item anterior;
- Pontos de vista controversos – Opiniões sobre racismo, religião, visões políticas, podem ser usados contra o próprio usuário.

Os pontos citados são extremamente importantes quando o assunto é proteção de identidade. Porém, o foco do artigo de Mattern é voltado para relações trabalhistas apenas. Assim, a seguir, é discutido como as informações extraídas de diversos pontos de um perfil social podem comprometer a segurança do usuário.

Um **perfil social** completo do Orkut possui locais para o usuário informar desde dados básicos sobre sua pessoa como nome, cidade, etc., como também dados adicionais como gostos pessoais, opção sexual, local onde mora, endereço do trabalho, escolas e cursos que já cursou, visões políticas e religiosas, entre outras. De posse desses dados, um engenheiro social ganha acesso ao íntimo da vítima, podendo usar contra elas em ataques como *phishing* e roubo de identidade.

O **álbum de fotos** guarda muito mais informações do que aparenta. Círculo interno de amigos, lugares onde o usuário frequenta, local de trabalho e hábitos pessoais podem ser deduzidos por um engenheiro social, colocando em risco a segurança do usuário.

A **lista de comunidades** a qual o usuário é filiado também pode oferecer dados importantes sobre a personalidade e os hábitos de um usuário. Uma prática bastante comum entre os usuários do Orkut, por exemplo, é se afiliar a “comunidades de afirmação”, como foi discutido em seção anterior. Essas comunidades não possuem o propósito de grupo de discussão, mas sim afiliar usuários que se enquadram no título da comunidade. Exemplos como “*Eu odeio acordar cedo”, “Eu adoro balada”, “Eu bebo até cair”, “Eu odeio meu trabalho”, “Eu adoro loiras”*, entre outras, podem oferecer informações extremamente precisas sobre a personalidade de um usuário.

Seus **comentários, bate-papos e depoimentos**, servem para um engenheiro social traçar uma lista dos amigos íntimos, marcação de encontros, compromissos e planos futuros

da vítima. Como citado na matéria dos falsos sequestradores, a análise das conversas de um usuário pode servir para planejar um golpe se aproveitando do *timing* e das informações privadas a qual o engenheiro teve acesso.

Em resumo, um perfil social completo de um usuário fornece a uma pessoa mal intencionada dados suficientes para atrair uma vítima para um golpe. De posse de informações sobre gostos pessoais, hábitos cotidianos, opiniões sobre diversos temas, círculo interno de amigos e locais onde o usuário frequenta constantemente, um engenheiro social possui, na ponta dos dedos, todos os dados que ele precisa para aplicar um golpe sem se expor.

Um caso noticiado pelo portal TechTudo, em julho de 2011, exemplifica um ataque de um engenheiro social por meio de um site de relacionamento:

> "George Bronk, 24 anos, foi condenado a quatro anos de cadeia por usar o Facebook para invadir a conta de muitas mulheres. O morador da Califórnia procurava, nos perfis da rede social, por pistas que o levassem a descobrir as senhas dos emails de suas vítimas. Assim que encontrava dados, o *hacker* invadia os computadores e procurava por conteúdo erótico. Bronk chegou a enviar imagens das mulheres a seus maridos, namorados e colegas de trabalho. O jovem hacker fez de vítimas mulheres em mais de 17 estados dos Estados Unidos." (TECHTUDO, 2011).

Outro exemplo que cita as brechas de segurança presente nas redes sociais foi noticiado no jornal Valor Econômico em 03/05/2010:

> "Recentemente, a empresa de segurança digital Check Point fez um teste para medir os riscos das redes sociais. De forma aleatória, selecionou uma amostra de usuários do Facebook para simular um ataque de "*phishing*". A técnica consiste em convidar o usuário a acessar uma página falsa - por vezes, imitando um site autêntico -, para roubar informações confidenciais. Depois de criar um perfil falso e anônimo no Facebook, a empresa distribuiu um email com uma frase comum nas mensagens de *spam* ou lixo eletrônico: "Venha ver minhas fotos mais recentes". O resultado mostrou que dos 200 usuários do Facebook que receberam a mensagem, 71 clicaram no endereço. Isto é, mais de um terço das pessoas tentaram acessar a página, sem ter a menor ideia do que se tratava o link ou de quem era o remetente." (BORGES, 2010).

Diante dos fatos supracitados, a confiança na segurança das redes sociais faz com que os usuários exponham mais do que deveriam, se tornando assim, alvos para golpistas que usam técnicas de engenharia social para cometer seus crimes.

No próximo capítulo, são descritos como os administradores de segurança das redes sociais tentam impedir esse tipo de ataque e quais as defesas que foram criadas nesses sites para diminuir o acesso a informações privadas.

3. A EVOLUÇÃO DOS PROCESSOS DE SEGURANÇA NAS REDES SOCIAIS

A segurança ao acesso a informações privadas dos usuários de redes sociais é um ponto que sofre constante investimento e esforço por trás dos administradores desses sites. Durante a expansão desses sites, a segurança foi um fator preponderante de evolução, tendo em vista as constantes ameaças que surgia a cada dia.

Como dito em seção anterior, quando os sites de relacionamento surgiram, o único obstáculo que impedia uma pessoa mal intencionada a ter acesso completo aos dados de outro usuário, resumia-se apenas a ser um membro da rede. O próprio Orkut seguia esse paradigma com os seus “convites”.

Para ser membro da rede do Orkut, um usuário precisava ser *convidado*. Não havia acesso livre a qualquer pessoa por meio de registro aberto. Por isso, partindo do princípio que alguém só convidaria outra pessoa se ela fosse de confiança, a segurança das informações dentro de um perfil social não era alta.

Tudo mudou com a concorrência e o surgimento de novas redes sociais. Quando o Google comprou o Orkut, a primeira medida tomada para aumentar o uso da rede social foi abrir a possibilidade de ser membro para qualquer usuário que tivesse conta no Gmail (email da Google). Esse método para aumentar a audiência funcionaria em mão dupla: de um lado, todos os membros do Orkut teriam contas do Gmail e do outro, qualquer usuário de Gmail agora podia ser membro do Orkut.

Esse último ponto fez com que, tecnicamente, o Orkut se tornasse aberto ao público, sem necessidade de convite. Bastava abrir uma conta no Gmail e você faria parte da rede do Orkut.

Para um público de membros que estavam acostumados apenas com “usuários convidados” acessando aos seus perfis, essa “enxurrada” de novos usuários abriu uma enorme brecha de privacidade e segurança. O *habitat* seguro desses usuários começou a se tornar hostil.

A abertura do acesso público ao Orkut coincidiu com o aumento de casos de *phishing*, roubo de identidade e quebra de identidade. Foi por meio do aumento dessas ameaças e das experiências bem sucedidas em outras redes sociais, que em 2008, o Orkut implementou um sistema de permissões de acessos.

Esse sistema de permissões é padrão nas outras redes sociais mais utilizadas, como Facebook e Myspace. Ela se baseia na mesma prerrogativa dos sistemas de permissões de outras redes utilizadas por um grupo de pessoas: um usuário só tem acesso a determinada informação se for liberado pelo próprio administrador da rede.

No caso das redes sociais, o “administrador” é o usuário dono da conta. A diferença entre o sistema de permissões de redes convencionais para o das redes sociais é que o número de usuários é muito grande para se “administrar” a nível individual.

Por isso, as redes sociais (incluindo o Orkut) trabalham com essas permissões em nível de grupo: Todas as informações pessoais, fotos, vídeos e bate papos, são disponíveis para visualização apenas para outros membros marcados como “amigos”. O acesso vai caindo de abrangência conforme a marcação do membro for caindo de nível (“colega”, “conhecido”, “trabalho”, “não conheço”). Também é possível ao usuário criar grupos específicos, adicionar membros de sua lista nesses grupos e atribuir permissões específicas.

Por exemplo, um usuário pode criar um grupo chamado “Parentes”, adicionar todos os membros da sua lista que, segundo ele, pertencem a este grupo e bloquear o acesso a fotos que são liberadas, por exemplo, para o grupo “Amigos Íntimos”.

Como suporte a este novo sistema de permissões, todas as informações postadas pelo usuário na rede social também precisam receber uma marcação informando que tipo de permissão um membro precisa ter para acessar aquele *post*. Ainda seguindo o exemplo acima, um vídeo marcado com a permissão “apenas para o grupo Amigos Íntimos” não seria sequer listado como disponível para os membros do grupo “Parentes”.

Além do sistema de permissões, o Orkut implementou o uso de *captchas* (confirmação por escrita) em diversas áreas de sua interface. Uma mensagem contendo links externos que é postada num *scrapbook* de outro usuário ou numa discussão de uma comunidade precisa passar por um captcha antes de ser enviada. Isso foi implementado visando reduzir ou a impedir o uso de *bots* (programas de postagem em massa) e de *spammers*.

Outro uso de *captchas* visa reduzir os *mass friendlers*, programas automatizados que adiciona amigos a sua lista de forma automática. A partir do décimo convite de amizade lançado por um usuário num curto espaço de tempo (30 minutos), *captchas* começaram a aparecer em frequência maior, requerendo uma interação física do usuário. A partir do trigésimo convite lançando em menos de meia hora, haverá um novo *captcha* que precisará ser confirmado a cada novo convite.

Por último, dentro das configurações de segurança do Orkut, há a opção de habilitar uma confirmação de email para membros que lancem convites de amizade para você. O

modelo padrão de convite só contém uma frase: "[nome do membro], você quer ser meu amigo no Orkut? Ass.: [nome do usuário]". Com essa confirmação habilitada, outro campo aparece embaixo do convite obrigando o membro a informar seu email de contato.

No próximo capítulo, esses sistemas de segurança são analisados com relação à usabilidade, clareza e eficácia.

4. ESTUDOS DE CASO

O processo de experimentação deste estudo foi feito em duas etapas, ambas de forma relacionada e consequencial.

A primeira delas se baseou na criação de dois perfis falsos dentro da rede do Orkut. Ambos os perfis foram utilizados para testar a interação entre dois usuários das mais diversas maneiras, emulando situações cotidianas entre dois usuários distintos dentro da rede. Essas situações cotidianas envolvem convidar como amigo, enviar mensagens, postar fotos, administrar permissões e grupos etc. O objetivo dessa etapa visou analisar os sistemas de segurança do Orkut, sua usabilidade, clareza e eficácia.

A segunda etapa surgiu como decorrência das falhas de segurança encontradas na primeira etapa. Os dois perfis falsos receberam atualizações para se parecem com perfis verdadeiros de usuários reais. Essas atualizações incluíam a adição de fotos nos perfis, postagens fictícias marcadas com diversos tipos de permissão, a adição de comunidades relacionadas à personalidade fictícia desses dois usuários e por fim, o preenchimento completo do "perfil pessoal" com dados e endereços falsos.

Ambos os perfis foram marcados com a sigla RLC no final dos seus nomes como referência ao autor deste trabalho.

Fig. 2: Perfil de "Priscila Miranda", primeiro usuário criado para a experimentação.

O primeiro perfil mostrado na Figura 2, da usuária "Priscila Miranda" (doravante chamada de *primira12*), foi criado visualizando uma mulher de 20 anos, solteira, estudante, paulista e católica. As comunidades que o usuário *primira12* participa são: "*Tom Jobim*", "*Marisa Monte*", "*Eu usava aparelhos*", "*Love*" e "*Mãe eu te amo muito*!". No seu álbum de fotos há apenas uma foto de "Pluto", seu cachorro de estimação.

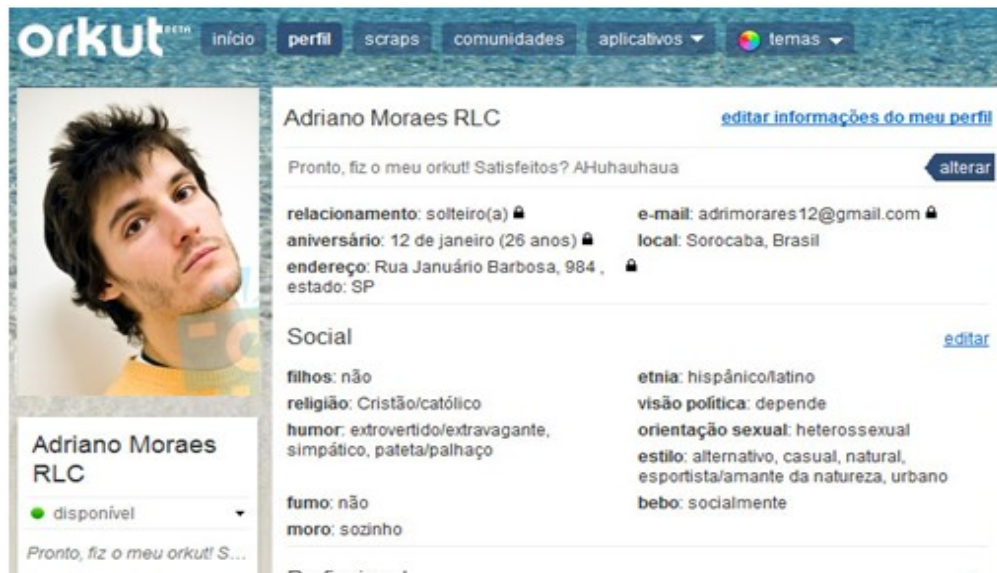



Fig. 3: Perfil de "Adriano Moraes", segundo usuário criado para a experimentação.

O segundo perfil mostrado na Figura 3, do usuário "Adriano Moraes" (doravante chamado de *adrimoraes12*), foi criado visualizando um homem de 26 anos, solteiro, estudante, paulista e católico. As comunidades que o usuário *adrimoraes12* participa são: "*Eu adoro McDonald's*", "*Campimg Brasil*", "*Formula 1 Brasil*", "*Caetano Veloso*" e "*Escalada* e *Rapel*". No seu álbum de fotos há fotos de pessoas praticando rapel e há um vídeo onde supostamente o usuário aparece praticando o esporte.

A partir de cada perfil, 50 convites de amizade foram lançados para usuários reais do Orkut, 25 homens e 25 mulheres de diferentes faixas etárias. No total, 100 convites foram lançados, 50 para usuários do sexo masculino e 50 para usuários do sexo feminino.

Os convites enviados foram os do modelo padrão, informado no capítulo anterior. Não houve nenhuma tentativa de facilitar a aceitação de um convite por meio de contatos ou tentativas subsequentes.

Todos os 100 usuários foram escolhidos aleatoriamente dentro do painel de membros da comunidade "Brasil". Esta comunidade foi escolhida por apresentar maior diversidade em

usuários de ambos os sexos, faixa etária, localização e grau de escolaridade (quando informados).

Foi dado um prazo de um mês para os convites enviados pelos dois perfis serem aceitos ou rejeitados. Após esse prazo, foi feito a tabulação das informações disponíveis nos perfis que aceitaram o convite. As informações analisadas foram:

- **Perfis** – Nome, idade, local de residência e trabalho, estado civil e outros dados pessoais que possam oferecem uma identificação positiva de uma pessoa.
- **Fotos pessoais** – Hábitos sociais, amigos íntimos, parentes, relacionamentos e locais de visita constante, como trabalho, escola, local de férias.
- **Comunidades** – Gostos pessoais, hábitos, opção sexual, locais de visita constante do usuário (escolas, boates, faculdades).

Cruzando os dados encontrados com as referências de perigo a privacidade citadas por Mitnick (2004), Mattern (2010) e Laribee (2006), foi criado um "ranking de periculosidade" no qual cada perfil social foi enquadrado. Este ranking possui uma escala de um a quatro. Os níveis desse ranking são explicados abaixo.

- **Grau 1:** Perfis sem nenhuma informação específica sobre o usuário. Difícil definir sexo, data de nascimento, local de residência e/ou trabalho.
- **Grau 2:** Perfis com referências indiretas sobre gostos pessoais, locais de trabalho, residência ou estudo nas comunidades afiliadas, *scrapbooks* ou álbum de fotos. Ex.: Usuário inscrito em comunidades afirmativas ou possuir fotos que referenciem grupos musicais, times de futebol, atividades profissionais e/ou atividades de lazer.
- **Grau 3:** Perfis com referências diretas sobre família, hábitos pessoais, locais de trabalho, residência ou estudo nas comunidades afiliadas, álbuns de fotos e *scrapbooks*. Ex.: Álbum de fotos contém fotos e informações de parentes, fotos de local de trabalho, amigos próximos e locais de comum frequência.
- **Grau 4:** Perfis com dados específicos sobre usuários. Ex.: Que contenha endereço residencial, telefone residencial, email pessoal, celular e/ou código de endereço postal

As análises dos resultados das duas fases da experimentação são apresentadas nas próximas seções.

4.1 Análise dos sistemas de segurança dos perfis do Orkut

Como dito no Capítulo 5, o aumento de problemas com privacidade dos usuários fez com que o Orkut implementasse diversas medidas de segurança visando a aumentar o controle dos usuários sobre o que os membros da rede podem ter acesso nas informações postadas por eles.

A primeira e mais importante medida de segurança foi o estabelecimento de permissões, gerenciadas pelos próprios usuários donos dos perfis. A partir das permissões os usuários podem marcar níveis de acessos diferentes para diferentes grupos de usuários que acessam seu perfil pessoal, seu *scrapbook* e seu álbum de fotos.

Nos testes realizados para este estudo, verificou-se que o sistema funciona sem falhas. No momento que um membro recebe permissão de nível suficiente para ter acesso à determinada informação, ela aparece disponível no perfil do usuário. O sistema de permissões em grupo também funciona: fotos, vídeos e outras postagens que não são permitidas a um determinado grupo sequer aparecem como existentes no perfil do usuário.

É possível possuir um perfil recheado de informações detalhadas sobre todos os aspectos da vida de um usuário e permitir acesso a essas informações a apenas uma pessoa ou a um grupo. É possível inclusive postar informações que não são acessíveis a ninguém, a não ser o próprio usuário (o que paradoxalmente vai de encontro à razão pela qual postar determinada informação).

No entanto, por meio da experimentação, foi percebido um problema na usabilidade de tal sistema: ele é contra intuitivo. Ao invés de quando uma informação nova postada pelo usuário ser marcada com a permissão mais segura, ela aparece, por padrão, com uma permissão de grande abrangência.

A opção padrão para novas postagens habilita todos os membros na lista de amigos do usuário ter acesso à informação postada. Além disso, como mostra a Figura 4, a permissão já vem pré-ativada, reduzindo a importância dela como ferramenta de uso obrigatório.

Fig. 4: Exemplo de permissão pré-ativada e abrangente.

O mesmo padrão de pré-ativação é encontrado no *scrapbook*, nos vídeos e no próprio perfil pessoal. Como descrito anteriormente, isso é contra intuitivo, pois ao invés das permissões serem restritivas ou dependentes do usuário para marcá-las, elas já aparecem pré-ativadas em um nível bem abrangente, como está ilustrado na Figura 5.

Fig. 5: Outro exemplo de permissão pré-ativada.

Uma comparação prática sobre o significado dessa falha seria o mesmo que em um sistema de usuários da rede de uma empresa, todo novo usuário receber a permissão pré-ativada de Administrador e, só por meio da interferência ativa do responsável pela rede, a permissão ser alterada para uma menor. Em um cenário real, é exatamente o contrário que acontece.

O sistema de *captchas* também foi testado e se mostrou eficiente apenas para programas que precisam traduzi-los para prosseguir. Porém, no caso de uma pessoa real ativamente enviando *scraps* com links externos ou enviando convites em massa para outros membros, os *scraps* se tornaram apenas um leve incômodo. Devido à natureza dos *captchas* utilizados pelo Orkut, eles são de fácil dedução e usam poucas letras, não impedindo que uma pessoa real mal intencionada seja atrapalhada por eles, mas sim, retardada. Exemplo disso é

que mesmo com os *captchas* aparecendo com extrema frequência, os 100 convites de amigos necessários para a segunda fase da experimentação foram enviados em menos de 30 minutos.

Ficou claro então, nessa primeira fase, que as ferramentas passivas de segurança implementadas pelo Orkut são eficientes até certo ponto. Sem dúvida, um usuário externo tentando acessar dados de membros que não fazem parte de sua lista de amigos terá pouco sucesso na sua empreitada. No entanto, basta ser "amigo" de um membro e todos os dados adicionados por ele com a permissão de "visível para todos os amigos" se tornarão acessíveis.

Foi a partir dessa descoberta que a segunda fase dessa experimentação foi baseada.

4.2 Análise dos perfis acessados pelos usuários *primira12* e *adrimoraes12*

Apesar de não estar incluída no escopo deste estudo, a primeira pergunta respondida depois do término do prazo de espera para os convites serem aceitos ou rejeitados foi: quantas pessoas aceitariam um convite de amizade enviado por um completo estranho?

Como mostrado no gráfico 1, das 100 pessoas que receberam um pedido de amizade dos dois perfis falsos criados para este experimento, 51 membros da rede do Orkut aceitaram. Vale ressaltar que foram enviados apenas convites na sua forma mais básica e que não foram feitas segundas tentativas. Além disso, é necessário informar que das 100 pessoas convidadas, apenas 10 tinham habilitado o sistema de confirmação de email citado no Capítulo 4.

Nos gráficos 2 e 3 foram separados os membros que aceitaram o convite entre os dois usuários (*primira12* e *adrimoraes12*) como também entre homens e mulheres.

Gráficos 2 e 3. Porcentagem de usuários que aceitaram os convites divididos entre homens e mulheres.

Enviados pelo usuário primira12

26%
34%
40%

Homens
Mulheres
Não Aceitaram

Enviados pelo usuário adrimoraes12

20%
8%
72%

50 convites enviados, 37 aceitos.
17 homens, 20 mulheres

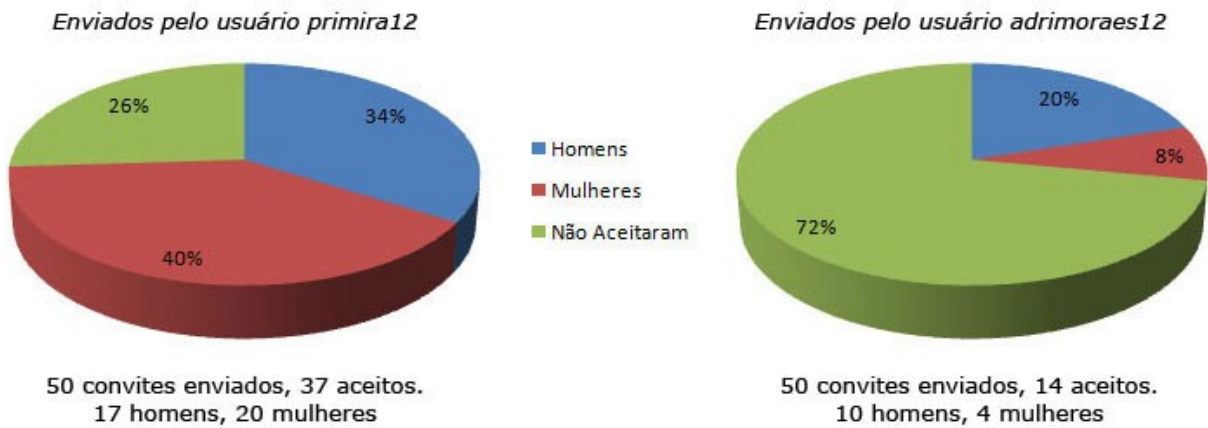
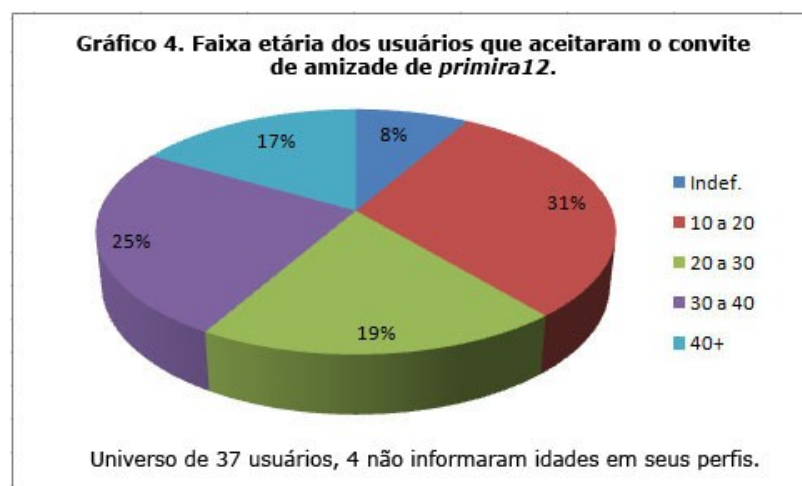
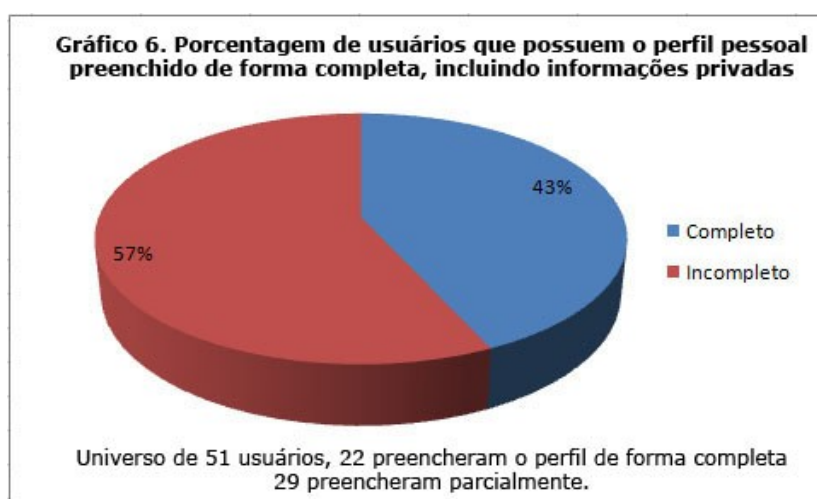
50 convites enviados, 14 aceitos.
10 homens, 4 mulheres

Vários pontos interessantes surgem: A usuária *primira12* obteve quase o triplo de convites aceitos em comparação ao usuário *adrimoraes12*. Foram 37 convites aceitos contra apenas 14, respectivamente. Outro ponto interessante é que enquanto os convites enviados por *primira12* foram aceitos de forma quase equivalente entre ambos os sexos (ligeira vantagem das mulheres), nos convites enviados por *adrimoraes12*, o número dos homens que aceitaram convites foi quase o dobro. Um último ponto que merece menção é o fato de que ambos os perfis tiveram mais sucesso em ter seus convites aceitos por membros do mesmo sexo que eles.

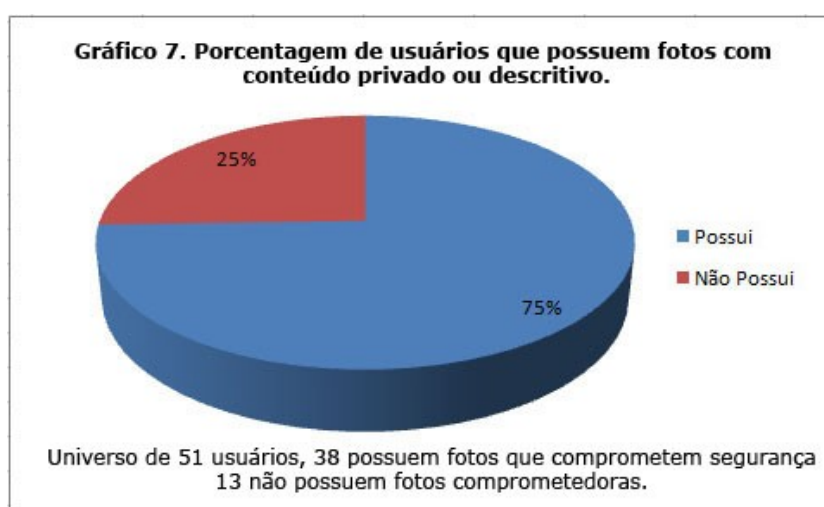
Gráfico 4. Faixa etária dos usuários que aceitaram o convite de amizade de *primira12*.

Universo de 37 usuários, 4 não informaram idades em seus perfis.

O gráfico 4 mostra a distribuição de faixa etária entre os usuários que aceitaram os convites do perfil *primira12*. Dentro de um universo de 37 usuários, onze tinham entre 10 a 20 anos, sete entre 20 a 30 anos, nove entre 30 a 40 anos e seis tinham mais de 40 anos. Quatro perfis pessoais não informavam a idade do usuário.

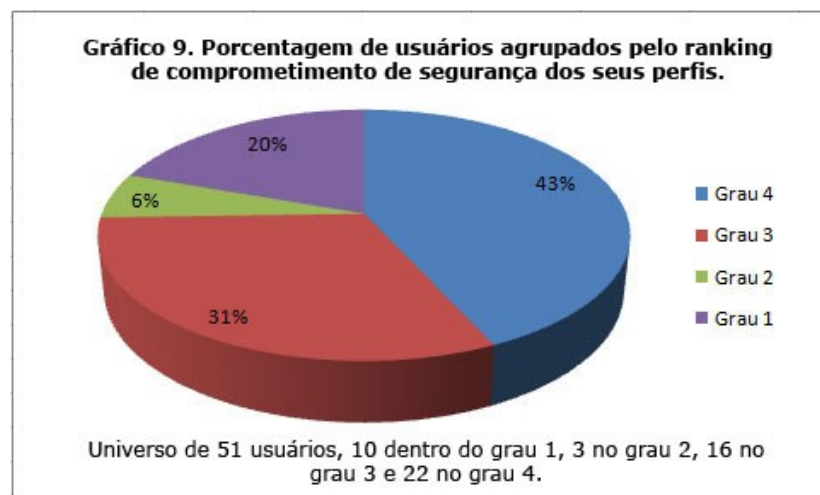
O gráfico 5 mostra a distribuição de faixa etária entre os usuários que aceitaram os convites de amizade do perfil *adrimoares12*. No universo de 14 usuários, três tinham entre 10 a 20 anos, cinco entre 20 a 30 anos, três entre 30 a 40 anos e três com mais de 40 anos. Em ambos os gráficos é possível perceber uma distribuição homogênea das idades, o que indica que não existe um determinante etário entre os usuários que aceitaram os convites de amizade.

O passo seguinte da experimentação foi analisar detalhadamente os 51 perfis à procura de informações pessoais, dados específicos sobre local de residência, trabalho ou estudo ou outras informações privadas que, nas mãos de um engenheiro social, poderia ser usado contra os usuários.

O gráfico 6 mostra o "perfil pessoal", também conhecida como a "folha de rosto" das contas dos 51 usuários. Do universo analisado, 22 membros (43%) possuíam o seu perfil preenchido de forma completa, contendo informações específicas sobre os pontos citados anteriormente com permissões abertas para "todos os amigos". Por outro lado, os outros 29

(57%) usuários preencheram os perfis apenas de forma parcial ou habilitaram permissões mais restritivas.

Alguns casos merecem menção: alguns usuários, além de preencherem completamente os seus perfis, ainda colocaram endereço residencial completo com o número da casa e o CEP. Outros usuários também disponibilizaram dados sigilosos como emails pessoais e endereços de contas de bate papo. Outro membro, um jovem de 17 anos, postou seu telefone celular e o da sua residência. Por último, há o caso de um rabino, que além de informar todos os dados citados acima, ainda postou o endereço da sinagoga onde trabalha.

No gráfico 7 é possível perceber que ao analisar os álbuns de fotos e vídeos dos 51 usuários, 75% deles possuíam algum tipo de foto ou vídeo, ou mesmo suas descrições, que caracterizavam uma brecha de segurança. Não há casos específicos a serem mencionados, pois todos seguem o mesmo padrão: parentes são nomeados, amigos íntimos são informados, locais de visitação constante como bares, boates, faculdades e escolas aparecem em destaque. Mesmo que os perfis pessoais desses usuários estivessem incompletos, as informações extraídas das fotos seriam o suficiente para colocar essas pessoas em riscos.

No gráfico 8, é possível perceber que uma porcentagem similar de usuários estão com a segurança dos seus perfis comprometidas por meio do excesso de comunidades descritivas as quais são afiliados. Dos 51 usuários que aceitaram os convites de amizade, 41 deles (80%) são afiliados a comunidades descritivas o suficiente para montar um perfil psicológico dessas pessoas. Há casos em que um único usuário é afiliado a mais de 400 comunidades, que, na grande maioria, são comunidades afirmativas como "*Eu estudo no Colégio Anglo*", "*Todo sábado vou na balada*" ou até mesmo "*Eu bebo até cair*".

Por último, os 51 perfis foram analisados na sua totalidade e foram agrupados por graus de comprometimento segundo o ranking elaborado na metodologia deste estudo.

Neste gráfico, é possível perceber que dos 51 usuários que aceitaram os convites, apenas 10 possuíam um perfil pessoal que não oferecesse riscos. Esses perfis possuíam poucas fotos, poucas comunidades afiliadas e poucas informações pessoais. Por outro lado, 41 perfis possuíam algum tipo de comprometimento: três possuíam riscos do **Grau 2**, por meio do qual um engenheiro social pode obter informações genéricas sobre a pessoa. Dezesseis estavam no **Grau 3**, no qual os dados fornecidos indicam locais de estudo, trabalho ou residência, como também o de parentes e amigos. No **Grau 4**, no entanto, foi onde se encaixou quase metade dos membros convidados (43%). Esses perfis ofereciam o maior grau de risco, com informações detalhadas sobre endereço residencial, lista de amigos íntimos, local de trabalho, números de telefone e email pessoais.

5. CONCLUSÃO

Como disse Mitnick (2004) no seu livro *A Arte de Enganar*, o problema da engenharia social é difícil de ser resolvido pois não está agregado ao código de programação ou ao *hardware* da máquina, mas sim às falhas inerentes ao comportamento humano que podem ser exploradas.

Durante este estudo foi visto que a maior parte dos problemas gerados pela engenharia social nos sites de relacionamento poderia ser evitada se tanto o usuário quanto a plataforma tivessem, como ponto de partida, a ideia de que a segurança das informações é essencial.

É claro que existem diversos fatores culturais, sociais e tecnológicos envolvidos, que, apesar de não ser do escopo deste estudo, interferem fundamentalmente na busca de uma solução para o problema. Além do mais, como disse o próprio Mitnick, enquanto o ser humano for o elo mais fraco da corrente de segurança, a brecha sempre vai existir. Segundo o próprio autor, "não existe *patch* para a estupidez humana". Por mais que essa afirmação soe pesada, o fato de ela vir de um dos engenheiros sociais mais procurados pela polícia americana na década de 90 faz com que ela, pelo menos, mereça relevância.

Apesar de tudo, mesmo que seja um fato de que a questão da engenharia social é um problema sem solução, durante o desenvolvimento deste estudo, alguns procedimentos e ações foram percebidas, que, se fossem implementados, poderiam reduzir consideravelmente o problema.

Do lado técnico da plataforma (neste caso o Orkut), a questão da "ineficácia" do sistema de permissões poderia ser resolvida se o problema da contra intuitividade fosse erradicado. Ao invés de ter como pré-definida uma permissão global de grande abrangência, o ideal seria se as permissões viessem com uma abrangência restrita, ou, melhor ainda, se a escolha das permissões viesse como um passo subsequente ao envio das postagens. O fato de usuário participar ativamente do controle de permissões reduziria consideravelmente a possibilidade de todas as informações postadas por um usuário ser de acesso livre a "todos os amigos".

Outro ponto dentro da plataforma que poderia ser melhorado é a questão dos *captchas*. Por mais que a eficácia deles esteja direcionada aos programas de mensagens em massa, eles deveriam vir acompanhados de outras restrições de navegabilidade para impedir que um usuário mal intencionado consiga executar ações suspeitas dentro de uma rede. Um exemplo

de uma ação suspeita seria enviar convites para 100 membros de uma única comunidade em meia hora. Um limitador de tempo ou uma limitação de número de amigos por dia atrapalharia ações como essa de forma um pouco mais eficaz.

É claro que nessas "soluções" não está sendo levada em conta a questão da praticidade ou da facilidade de uso por parte de usuário, nem questões comerciais e de marketing como número de usuários e a concorrência com outras redes. No entanto, a segurança não deve ser deixada para segundo plano em favor de "praticidade de uso" ou *share* de mercado.

O outro lado da moeda, o fator humano, é bem mais complicado de se resolver. A segunda fase da experimentação deixou esse problema evidente. Além do fato de que 50% dos perfis convidados por desconhecidos aceitaram a solicitação, apenas 10 desses perfis estavam livres de qualquer comprometimento de informações. Ficou evidente também que a falta de segurança não atinge especificamente nenhum sexo ou faixa etária em particular, sendo distribuído homogeneamente entre a maioria dos perfis.

Isso deixa evidente que, independentemente das questões sociais, culturais e econômicas, o pouco conhecimento da ferramenta e da tecnologia favorece o aparecimento de falhas nas mais bem arquitetadas plataformas.

No Brasil, esse problema se agrava ainda mais, pois o formato na qual a inclusão digital se apóia é fundamentalmente material: os investimentos dos governos se focam apenas em abrir o acesso da população aos meios tecnológicos, como corte de impostos, a diminuição de preços de equipamentos eletrônicos e a abrangência da cobertura de banda larga. No entanto, pouco é visto com relação ao investimento da educação tecnológica. Nas escolas onde existe instrução na área de Informática, o foco é direcionado a "como a tecnologia funciona", mas pouco é visto sobre "como usar bem a tecnologia".

O Brasil possui 79 milhões de internautas, quase metade da população nacional segundo dados do Ibope Nielsen (2011), porém, poucos desses usuários possuem qualquer formação básica sobre Segurança da Informação.

Fica evidente então que, da maneira como se apresenta, a batalha para a proteção de dados privados está fadada ao fracasso. Por mais que certas implementações dentro da plataforma sejam necessárias para garantir maior segurança dos dados divulgados, nada disso irá funcionar sem uma participação ativa de todas as esferas da sociedade, sejam elas políticas, educacionais ou familiares.

Apesar do processo de inclusão digital ter conseguido transformar o Brasil no quinto país com o maior número de internautas, nada disso vale se não houver uma conscientização, desde cedo, sobre a necessidade da segurança de dados pessoais.

São lições simples que podem ser dadas em sala de aula. Lições como "nunca divulgue numa rede de milhões de pessoas algo que você considera privado", "nunca publique dados específicos sobre sua pessoa" e "nunca, jamais aceite o convite de amizade de uma pessoa que você nunca viu na vida".

REFERÊNCIAS

24HORASNEWS. Bandidos usam dados do Orkut para planejar falsos seqüestros. (2006) <http://www.24horasnews.com.br/index.php?mat=175476> Acessado em 12/08/2011

ALEXA.COM, (2011) Orkut.com Site Info. Estatísticas de Visitação. <http://www.alexa.com/siteinfo/ orkut.com> Acessado em 15/08/2011

BARNES, Susan B. (2006). "A privacy paradox: Social networking in the United States". First Monday. <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle /1394/1312 > Acessado em: 13/08/2011

BORGES, André. Golpes da Web Migram para as redes sociais. (2010). Valor Econômico. <http://www.abmn.com.br/img/eventos/pdf2010/maio2/Golpes%20em%20redes %20sociais.pdf > Acessado em 14/08/2011

BORNATOVSKI, Eros; SILVA, Peterson; CARLA, Diane; CAMILLO, Samuel A.; POMBEIRO, Orlei (2006). Invasão de Privacidade por meio de Rastreamento de Informação. Sociedade Paranaense de Ensino e Informática.

BOYD, Danah; ELLISON, Nicole (2007). "Social Network Sites: Definition, History, and Scholarship". Journal of Computer-Mediated Communication 13.

COLLINS, Brendan (2008.) Privacy and Security Issues in Social Networking. FastCompany.com <http://www.fastcompany.com/articles/2008/10/social-networking-security.html> Acessado em 15/08/2011

COMSCORE, Orkut Continues to Lead_Brazil's Social Networking Market. (2010). <http://www.comscore.com/Press_Events/Press_Releases/2010/10/Orkut_Continues_to_Lead _Brazil_s_Social_Networking_Market_Facebook_Audience_Grows_Fivefold>, Acessado em 08/08/2011.

ELKINS, Sarah, (2007). A Social Network’s Faux Pas?. Newsweek.com, Newsbeast. <http://www.thedailybeast.com/newsweek/2007/11/08/a-social-network-s-faux-pas.html> Acessado em 16/08/2011.

ELLISON, N., LAMPE, C., STEINFIELD, C., & VITAK, J. (2009). A networked self: Identity, community and culture on social network sites. New York: Routledge.

FELITTI, Guilherme. Orkut: as razões para o sucesso da rede social do Google entre brasileiros. (2008). Ministério da Cultura. <http://www.cultura.gov.br/site/2008/07/10/orkut-as-razoes-para-o-sucesso-da-rede-social-do-google-entre-brasileiros/> Acessado em 12/08/2011

FOLHA DE SÃO PAULO, 2005. Orkut não entende seu sucesso no Brasil. <http://www1.folha.uol.com.br/folha/dinheiro/ult91u97858.shtml > Acessado: 02/08/2011.

GOODCHILD, Joan. (2010). Social Engineering: The Basics. Data Protection. <http://www.csoonline.com/article/514063/social-engineering-the-basics> Acessado em 02/08/2011.

HAUBEN, Michael & HAUBEN, Melinda. The Net and the Netizens. (1995). Columbia University. <http://www.columbia.edu/~rh120/ch106.x01 > Acessado em 01/08/2011.

HUFFAKER, David A.; CALVERT , Sandra L., (2005). “Gender, identity, and langugage use in teenage blogs,” Journal of Computer–Mediated Communication, (volume 10, number 2), <http://jcmc.indiana.edu/vol10/issue2/huffaker.html>, Acessado em: 15/08/2011.

KNAPP, E. (2006). A Parent's Guide to Myspace. DayDream Publishers

LARIBEE, Lena. Development of Methodical Social Engineering Taxonomy Project. (2006). Naval Postgraduate School. <http://faculty.nps.edu/ncrowe/oldstudents/laribeethesis.htm> Acessado em 12/08/2011.

MATTERN, Jennifer. 5 Things to Keep Off Social Networking Profiles. (2010). Social Implications. <http://socialimplications.com/5-things-to-keep-off-social-networking-profiles-if-youll-ever-be-job-hunting-again/ > Acessado em 13/08/2011

MITNICK, Kevin. A Arte de Enganar. (2004). Pearson. 1ª Edição.

ROSENBLUM, David, (2007). "What Anyone Can Know: The Privacy Risks of Social Networking Sites," IEEE Security and Privacy, vol. 5, no. 3.

TECHTUDO, Homem que usou o Facebook para perseguir mulheres em 17 estados é condenado. (2011) < http://www.techtudo.com.br/noticias/noticia/2011/07/homem-que-usou-o-facebook-para-perseguir-mulheres-em-17-estados-e-condenado.html> Acessado em 13/08/2011.

THE REGISTER, Office workers give away passwords for a cheap pen. (2003) <http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/ > Acessado em 12/08/2011